Australian Government

Department of Education, Employment and Workplace Relations

PRSTS303A Test installed security equipment/system

Release: 1

PRSTS303A Test installed security equipment/system

Modification History

Not applicable.

Unit Descriptor

This competency standard covers the skills and knowledge required to test a range of security equipment and systems including cable systems, equipment components and programming. It requires the ability to select and carry out tests suitable to confirm the integrity, security and safety of the security equipment/system. Competency also requires the ability to interpret and accurately document the test results. This work applies in extra low voltage as defined through the Australian Standards As 2201 (1986) environments and would be carried out under routine supervision within organisational guidelines.
Functional Area: Core, Technical Security
This competency standard covers the skills and knowledge required to test a range of security equipment and systems including cable systems, equipment components and programming. It requires the ability to select and carry out tests suitable to confirm the integrity, security and safety of the security equipment/system. Competency also requires the ability to interpret and accurately document the test results. This work applies in extra low voltage as defined through the Australian Standards As 2201 (1986) environments and would be carried out under routine supervision within organisational guidelines.
Functional Area: Core, Technical Security

Application of the Unit

Not applicable.

Licensing/Regulatory Information

Not applicable.

Pre-Requisites

Not applicable.

Employability Skills Information

Not applicable.

Elements and Performance Criteria Pre-Content

Not applicable.

Elements and Performance Criteria

Elements and Performance Criteria

Element	Performance Criteria
1 Prepare for testing	1.1 Work order is reviewed and clarified with appropriate person(s) as required in accordance with organisational requirements
	1.2 Type and location of security equipment / system to be tested is identified and checked against the work order
	1.3 Testing parameters are identified and confirmed in accordance with manufacturer's specifications
	1.4 Tools, equipment and materials are selected appropriate to job requirements and checked for operational effectiveness in accordance with manufacturer's specifications and organisational procedures
	1.5 Potential and existing risks and hazards involved with testing security equipment / systems are identified and managed in accordance with OHS policies and procedures and organisational requirements
	1.6 Suitable personal protective equipment is selected, used and maintained in accordance with OHS and organisational requirements
2 Test security equipment / system	2.1 Safe operating practices are observed to remove risk of injury to self, others or security equipment / system in accordance with OHS and organisational requirements
	2.2 Parts or connections of security equipment / system are removed as required in accordance with manufacturer's specifications and safely stored to protect against loss or damage
	2.3 Tests are conducted in accordance with manufacturer's specifications and provide reliable

	and accurate test data on the operation and functioning of security equipment / systems
	2.4 Security equipment / system is reassembled as required and returned to pre-test conditions in accordance with manufacturer's specifications
	2.5 Personal limitations in conducting testing are promptly identified and assistance is sought from appropriate person(s) in accordance with organisational procedures
3 Complete testing	3.1 Tests results are accurately recorded and relevant documentation is completed and processed in accordance with legislative, industry and organisational requirements
	3.2 Notification of work completion is made to appropriate person(s) in accordance with organisational procedures
	3.3 Malfunctions or deficiencies in the operation of security equipment / system and / or components are reported in accordance with industry standards and organisational procedures
	3.4 Work area, tools and equipment are cleaned and stored in a secure and safe location in accordance with organisational requirements
	3.5 Waste from testing activities is collected, treated and disposed of or recycled in accordance with organisational procedures and environmental policies

Required Skills and Knowledge

Not applicable.

Evidence Guide

The Evidence Guide identifies the requirements to be demonstrated to confirm competence for this unit. Assessment must confirm sufficient ability to use appropriate skills and knowledge to test installed security equipment/systems. Assessment of performance should be over a period of time covering all categories within the Range of Variables statements that are applicable in the learning environment.

What critical aspects are required for evidence of competency?

Identify testing parameters appropriate to type of security equipment/system and organise appropriate tools, equipment and materials to carry out testing procedures.

Select and carry out suitable tests and methods to check and confirm security equipment/system performance and operational effectiveness.

Prepare and submit correctly interpreted test results and other relevant documentation in a prompt and accurate manner.

Reinstate work area to pre-test condition and clean and safely store tools and equipment.

What specific knowledge is needed to achieve the performance criteria?

Knowledge and understanding are essential to apply this standard in the workplace, to transfer the skills to other contexts and to deal with unplanned events. The knowledge requirements for this competency standard are listed below:

powering systems types, functions and requirements of security equipment/systems
keypad and control panel types and functions
types and functions of tools and equipment
isolating and testing procedures
cable identification techniques
earthing systems, arrangements and requirements
electrical concepts (voltage, current, resistance and impedance)
electrical connections and types of electrical circuits
circuit protection requirements
cable handling requirements
computer software types and functions
technical terminology
organisational and client confidentiality requirements
OHS requirements and safe work practices
Requirements for compliance with Australian building codes and regulations and Australian Communications Authority (ACA) cabling standards.

What specific skills are needed to achieve the performance criteria?

To achieve the performance criteria, some specific skills are required. These include the ability to:

read and interpret plans and specifications
communicate in a clear and concise manner
select and use relevant testing tools and equipment
test security equipment/systems
evaluate test results
identify, isolate, test and tag cables
power security equipment/system
download and upload information
use keypads and control panels
methodically prioritise and organise work tasks

solve routine problems
estimate resource requirements
apply safe and efficient work practices.

What resources may be required for assessment?

Access to a suitable venue and equipment.
Access to plain English version of relevant statutes and procedures.
Assignment instructions, work plans and schedules, policy documents and duty statements.
Assessment instruments, including personal planner and assessment record book.
Access to a registered provider of assessment services.

What is required to achieve consistency of performance?

For valid and reliable assessment of this unit, the competency should be demonstrated over a period of time and observed by the assessor. The competency is to be demonstrated in a range of situations, which may include involvement in related activities normally experienced in the workplace.
Evidence of underpinning knowledge understanding of processes and principles can be gained through thorough questioning and by observation of previous work.

Assessment against this unit may involve the following:

Continuous assessment in a setting that simulates the conditions of performance described in the elements, performance criteria and range of variables statement that make up the unit.
Continuous assessment in the workplace, taking into account the range of variables affecting performance.
Self-assessment on the same terms as those described above.
Simulated assessment or critical incident assessment, provided that the critical incident involves assessment against performance criteria and an evaluation of underpinning knowledge and skill required to achieve the required performance outcomes.

Key competency levels

There are a number of processes that are learnt throughout work and life which are required in all jobs. They are fundamental processes and generally transferable to other work functions. Some of these are covered by the key competencies, although others may be added. Information below highlights how these processes are applied in this competency standard.

1 - perform the process
2 - perform and administer the process
3 - perform, administer and design the process

How can **communication of ideas and information** be applied? (**2**)

Notification may be made to relevant persons upon the completion of testing procedures of security equipment/systems.

How can **information be collected**, **analysed and organised**? (**2**)

Tests results may be interpreted, accurately recorded and organised in suitable formats for analysis.

How are **activities planned and organised**? (**2**)

Security equipment/systems for testing may be accessed with minimal disruption to client services, property or normal work routines.

How can **team work** be applied? (**2**)

Personal limitations in carrying out testing procedures may be promptly identified and assistance sought from relevant persons.

How can the use of **mathematical ideas and techniques** be applied? (**2**)

Mathematical techniques may be used to accurately estimate resource requirements and prioritise work tasks.

How can **problem solving skills** be applied? (**2**)
Malfunctions or deficiencies in the operation of security equipment/system and/or components are promptly reported for remedial action.
How can the **use of technology** be applied? (**2**)
Technology may be used to communicate, source and record information. It may also be used to carry out testing activities.
The Evidence Guide identifies the requirements to be demonstrated to confirm competence for this unit. Assessment must confirm sufficient ability to use appropriate skills and knowledge to test installed security equipment/systems. Assessment of performance should be over a period of time covering all categories within the Range of Variables statements that are applicable in the learning environment.
What critical aspects are required for evidence of competency?
Identify testing parameters appropriate to type of security equipment/system and organise appropriate tools, equipment and materials to carry out testing procedures.
Select and carry out suitable tests and methods to check and confirm security equipment/system performance and operational effectiveness.
Prepare and submit correctly interpreted test results and other relevant documentation in a prompt and accurate manner.
Reinstate work area to pre-test condition and clean and safely store tools and equipment.
What specific knowledge is needed to achieve the performance criteria?
Knowledge and understanding are essential to apply this standard in the workplace, to transfer the skills to other contexts and to deal with unplanned events. The knowledge requirements for this competency standard are listed below:
powering systems types, functions and requirements of security equipment/systems
keypad and control panel types and functions
types and functions of tools and equipment
isolating and testing procedures
cable identification techniques
earthing systems, arrangements and requirements
electrical concepts (voltage, current, resistance and impedance)
electrical connections and types of electrical circuits
circuit protection requirements
cable handling requirements
computer software types and functions
technical terminology
organisational and client confidentiality requirements
OHS requirements and safe work practices
Requirements for compliance with Australian building codes and regulations and Australian Communications Authority (ACA) cabling standards.
What specific skills are needed to achieve the performance criteria?
To achieve the performance criteria, some specific skills are required. These include the ability to:
read and interpret plans and specifications
communicate in a clear and concise manner
select and use relevant testing tools and equipment
test security equipment/systems
evaluate test results
identify, isolate, test and tag cables

power security equipment/system
download and upload information
use keypads and control panels
methodically prioritise and organise work tasks
solve routine problems
estimate resource requirements
apply safe and efficient work practices.

What resources may be required for assessment?

Access to a suitable venue and equipment.
Access to plain English version of relevant statutes and procedures.
Assignment instructions, work plans and schedules, policy documents and duty statements.
Assessment instruments, including personal planner and assessment record book.
Access to a registered provider of assessment services.

What is required to achieve consistency of performance?

For valid and reliable assessment of this unit, the competency should be demonstrated over a period of time and observed by the assessor. The competency is to be demonstrated in a range of situations, which may include involvement in related activities normally experienced in the workplace.
Evidence of underpinning knowledge understanding of processes and principles can be gained through thorough questioning and by observation of previous work.

Assessment against this unit may involve the following:

Continuous assessment in a setting that simulates the conditions of performance described in the elements, performance criteria and range of variables statement that make up the unit.
Continuous assessment in the workplace, taking into account the range of variables affecting performance.
Self-assessment on the same terms as those described above.
Simulated assessment or critical incident assessment, provided that the critical incident involves assessment against performance criteria and an evaluation of underpinning knowledge and skill required to achieve the required performance outcomes.

Key competency levels

There are a number of processes that are learnt throughout work and life which are required in all jobs. They are fundamental processes and generally transferable to other work functions. Some of these are covered by the key competencies, although others may be added. Information below highlights how these processes are applied in this competency standard.

1 - perform the process
2 - perform and administer the process
3 - perform, administer and design the process

How can **communication of ideas and information** be applied? (**2**)

Notification may be made to relevant persons upon the completion of testing procedures of security equipment/systems.

How can **information be collected**, **analysed and organised**? (**2**)

Tests results may be interpreted, accurately recorded and organised in suitable formats for analysis.

How are **activities planned and organised**? (**2**)

Security equipment/systems for testing may be accessed with minimal disruption to client services, property or normal work routines.

How can **team work** be applied? (**2**)

Personal limitations in carrying out testing procedures may be promptly identified and assistance sought from relevant persons.

How can the use of **mathematical ideas and techniques** be applied? (**2**)

Mathematical techniques may be used to accurately estimate resource requirements and prioritise work tasks.

How can **problem solving skills** be applied? (**2**)

Malfunctions or deficiencies in the operation of security equipment/system and/or components are promptly reported for remedial action.

How can the **use of technology** be applied? (**2**)

Technology may be used to communicate, source and record information. It may also be used to carry out testing activities.

Range Statement

The Range of Variables provides information about the context in which the unit of competency is carried out. It allows for different work practices and work and knowledge requirements as well as for differences between organisations and workplaces. The following variables may be present for this particular unit:

Work order information may include:
work schedules
completion dates
job requirements and tasks
specific client requirements
access to site and specific site requirements
resource requirements
OHS requirements
compliance with relevant legislation
budget allocations
warranties and service information.

Appropriate person(s) may include:
clients
site managers, project managers
engineers and technicians
technical experts
line managers/supervisors
colleagues, security consultants
regulatory personnel.

Organisational requirements may relate to:
legal and organisational operational policies and procedures
operations manuals, induction and training materials
insurance policy agreements
client and organisational confidentiality requirements
organisational goals, objectives, plans, systems and processes
employer and employee rights and responsibilities
own role, responsibility and delegation
quality and continuous improvement processes and standards
client service standards
defined resource parameters
OHS policies, procedures and programs
emergency and evacuation procedures
duty of care, code of conduct, code of ethics
access and equity policy, principles and practice
records and information systems and processes
communication channels and reporting procedures.

Security equipment and systems may include:
detection devices, audible/visual warning devices
cameras, monitors and control equipment
control panels, intercoms
wireless equipment, car alarms
electronic readers, electronic recognition controls

locks and locking systems
grills, lighting, boom gates, turnstiles
bank pop-up screens
smoke detection devices
electric/mechanical fire safety and fire locking systems
power supplies, batteries
security doors and door controls.

Security systems may be:
electronic
mechanical
computerised
procedural.

Tests may involve/include:
cables
wiring and connections (continuity, resistance, earth leakage, voltage)
walk tests, coverage tests, safety tests, calibration tests
correct relaying of information/data
testing to specifications
detection tests, alarm tests, functional tests.

Tools and equipment may include:
computer, software
testing equipment
ladder, scaffold, scissor lift, hoist
batteries
personal protective equipment
communications equipment.

Materials may include:
computer disks
test board
test tape.

Manufacturers specifications may be found in:
printed instruction leaflets
operators manuals
equipment specifications
attachments to equipment
plans and diagrams
warranty documents.

Risks and hazards may include:
non-compliance with building codes and regulations
exposed electrical wiring
manual handling
chemical hazards (battery corrosion)
exposure to:
asbestos
dust
noise
live power
vermin

water
glass fibre
building debris
natural and other gas build-up.

OHS policies and procedures may relate to:
hazardous and risk assessment mechanisms
implementation of safety regulations
safety training
safety systems incorporating:
work clearance procedures
isolation procedures
gas and vapour
monitoring/testing procedures
use of protective equipment and clothing

use of codes of practice.

Personal protective equipment may include:
safety boots
masks
safety glasses
knee pads
gloves
first aid kid, fire extinguisher.

Safe operating practices may include:
working safely around electrical wiring, cables and overhead power lines
working safely around tools and equipment
hazard recognition
emergency procedures
awareness of electrical hazards
following confined spaces procedures
administering first aid.

Documentation may include:
work log
records of equipment/system positioning
section lists, zone lists, equipment lists
cable identification records, fixings, job card
records of any adjustments to original cable plan
records of faulty or malfunctioning tools and equipment
testing and inspection results
records of materials used
costings.

Applicable legislation, **codes and national standards may relate to**:
compliance with Australian building codes and regulations
compliance with Australian Communications Authority (ACA) cabling standards
relevant Commonwealth/State/Territory legislation which affect organisational operation:
Occupational Health and Safety and safe work practices
environmental issues
equal employment opportunity

industrial relations
anti-discrimination and diversity

licensing arrangements
Australian Standards, quality assurance and certification requirements
relevant industry Codes of Practice
award and enterprise agreements
trade practices
privacy requirements
freedom of information.

The Range of Variables provides information about the context in which the unit of competency is carried out. It allows for different work practices and work and knowledge requirements as well as for differences between organisations and workplaces. The following variables may be present for this particular unit:

Work order information may include:
work schedules
completion dates
job requirements and tasks
specific client requirements
access to site and specific site requirements
resource requirements
OHS requirements
compliance with relevant legislation
budget allocations
warranties and service information.

Appropriate person(s) may include:
clients
site managers, project managers
engineers and technicians
technical experts
line managers/supervisors
colleagues, security consultants
regulatory personnel.

Organisational requirements may relate to:
legal and organisational operational policies and procedures
operations manuals, induction and training materials
insurance policy agreements
client and organisational confidentiality requirements
organisational goals, objectives, plans, systems and processes
employer and employee rights and responsibilities
own role, responsibility and delegation
quality and continuous improvement processes and standards
client service standards
defined resource parameters
OHS policies, procedures and programs
emergency and evacuation procedures
duty of care, code of conduct, code of ethics
access and equity policy, principles and practice

records and information systems and processes
communication channels and reporting procedures.

Security equipment and systems may include:
detection devices, audible/visual warning devices
cameras, monitors and control equipment
control panels, intercoms
wireless equipment, car alarms
electronic readers, electronic recognition controls
locks and locking systems
grills, lighting, boom gates, turnstiles
bank pop-up screens
smoke detection devices
electric/mechanical fire safety and fire locking systems
power supplies, batteries
security doors and door controls.

Security systems may be:
electronic
mechanical
computerised
procedural.

Tests may involve/include:
cables
wiring and connections (continuity, resistance, earth leakage, voltage)
walk tests, coverage tests, safety tests, calibration tests
correct relaying of information/data
testing to specifications
detection tests, alarm tests, functional tests.

Tools and equipment may include:
computer, software
testing equipment
ladder, scaffold, scissor lift, hoist
batteries
personal protective equipment
communications equipment.

Materials may include:
computer disks
test board
test tape.

Manufacturers specifications may be found in:
printed instruction leaflets
operators manuals
equipment specifications
attachments to equipment
plans and diagrams
warranty documents.

Risks and hazards may include:
non-compliance with building codes and regulations
exposed electrical wiring

manual handling
chemical hazards (battery corrosion)
exposure to:
asbestos
dust
noise
live power
vermin
water
glass fibre
building debris
natural and other gas build-up.

OHS policies and procedures may relate to:
hazardous and risk assessment mechanisms
implementation of safety regulations
safety training
safety systems incorporating:
work clearance procedures
isolation procedures
gas and vapour
monitoring/testing procedures
use of protective equipment and clothing

use of codes of practice.

Personal protective equipment may include:
safety boots
masks
safety glasses
knee pads
gloves
first aid kid, fire extinguisher.

Safe operating practices may include:
working safely around electrical wiring, cables and overhead power lines
working safely around tools and equipment
hazard recognition
emergency procedures
awareness of electrical hazards
following confined spaces procedures
administering first aid.

Documentation may include:
work log
records of equipment/system positioning
section lists, zone lists, equipment lists
cable identification records, fixings, job card
records of any adjustments to original cable plan
records of faulty or malfunctioning tools and equipment
testing and inspection results
records of materials used

costings.
Applicable legislation, **codes and national standards may relate to**:
compliance with Australian building codes and regulations
compliance with Australian Communications Authority (ACA) cabling standards
relevant Commonwealth/State/Territory legislation which affect organisational operation:
Occupational Health and Safety and safe work practices
environmental issues
equal employment opportunity
industrial relations
anti-discrimination and diversity

licensing arrangements
Australian Standards, quality assurance and certification requirements
relevant industry Codes of Practice
award and enterprise agreements
trade practices
privacy requirements
freedom of information.

Unit Sector(s)

Not applicable.